IN THE CLAIMS

A1

1. (currently amended) A method for providing access to users based on user profiles and using a web-based system that includes a server system coupled to a centralized interactive database and at least one client system, said method comprising the steps of:

creating an electronic profile for a user within a centralized database;

creating an electronic profile for data within the centralized database;

establishing pre-determined rules and methodology for user access;

making a decision with reference to the user access after completing an evaluation based on the electronic profiles, pre-determined rules, and operating methodology in response to a request from the user for access; and

if the user is denied access, prompting the user to complete a request for quick approval wherein the request for quick approval is subjected to an internal exception access process, and quick approval is approved based on pre-established criteria.

2. (currently amended) A method according to Claim 1 wherein said step of creating an electronic profile for a user further comprises the step of creating an electronic profile based on information available from at least one an ~~OHR Application and an RFCA Application~~ Oracle Human Resource Application and a Request for Computer Access Application.

3. (original) A method according to Claim 1 wherein said step of creating an electronic profile for data further comprises the step of creating data profiles based on at least one of Data Elements, Data Tags, Rules of Access, an Approver's Name for Each Rule of Access, Rules of Exclusion, an Exception List, and Field Tags.

4. (original) A method according to Claim 3 wherein said step of establishing pre-determined rules and methodology for user access further comprises the steps of:

establishing pre-determined rules in the centralized database based on at least one of Rule Based Access guidelines, Group Based Access guidelines, Search & Subscribe

Utilities guidelines, Active Positioning Monitoring guidelines, Hard Exclusion Rules guidelines, and Access Audits guidelines; and

A1

establishing methodology to ensure timely and accurate decision making based on criteria established by the management.

5. (currently amended) A method for managing user profile information, including managing access control to applications and data by implementing a level of security across the different applications that is the same for each application, using a web-based system that includes a server system coupled to a centralized interactive database and at least one client system, said method comprising the steps of:

providing capabilities for a user to request access to information that the user currently does not have access to;

tracking a status of the request;

obtaining a decision from an owner of the data requested;

implementing the decision; ~~and~~

notifying the user of the decision ~~within a pre-determined time frame~~; and

if the user is denied access, prompting the user to complete a request for quick approval wherein the request for quick approval is subjected to an internal exception access process, and quick approval is approved based on pre-established criteria.

6. (original) A method according to Claim 5 wherein said step of obtaining a decision further comprises the step of obtaining at least one of an approval decision and a disapproval decision.

7. (original) A method according to Claim 5 wherein said step of implementing the decision further includes the steps of reviewing and auditing the user access.

8. (original) A method according to Claim 5 wherein said step of implementing the decision further includes the step of creating a consistent security model

that includes centralized administration of security of the system and uses single user profile and privilege for accessing different applications.

A1

9. (original) A method according to Claim 5 wherein said method further comprises the steps of:

creating user profiles;

providing access control to data associated with user profiles;

defining permissions based on a user identifier associated with user profiles; and

developing a specification for user interfaces.

10. (original) A method according to Claim 5 further comprising the step of providing administration of a common security model for access control and event notification.

11. (original) A method according to Claim 5 further comprising the step of updating profiles automatically on at least one of a pre-determined timed interval and a change in organization hierarchy.

12. (original) A method according to Claim 5 further comprises the step of updating profiles automatically when a user transfers departments.

13. (original) A method according to Claim 5 further comprising the step of generating access list reports that identify accessible and non-accessible data and restrictions for access.

14. (original) A method according to Claim 5 further comprising the step of retrieving information from the centralized database in response to a specific inquiry from an administrator.

15. (original) A method according to Claim 5 wherein the client system and the server system are connected via a network and wherein the network is one of a wide area network, a local area network, an intranet and the Internet.

16. (original) A database configured to be protected from access by unauthorized individuals by managing user and data profiles by an administrator, said database providing access to users based on pre-determined rules and criteria further comprising:

data corresponding to at least one of Rule Based Access guidelines, Group Based Access guidelines, Search & Subscribe Utilities guidelines, Active Positioning Monitoring guidelines, Hard Exclusion Rules guidelines, and Access Audits guidelines;

data corresponding to applications that cross-references the applications data against unique identifiers;

data corresponding to users that cross-references the users data against unique identifiers; and

data corresponding to various methodologies that facilitates accurate decision making.

17. (withdrawn) A web-based system for managing user profiles including access control to applications and data by implementing level of security across the different applications that is the same for each application, said system comprising:

a client system comprising a browser;

a data storage device for storing information;

a server system configured to be coupled to said client system and said database, said server system further configured to:

manage registration process by creating user profiles and data profiles;

manage Authorization Process by managing Default Access Process and Evaluation Process;

manage Maintenance Process by managing Exception Access Process and Access Process within the Data Storage Device.

A1

18. (withdrawn) A system according to Claim 17 wherein said data storage device further configured to:

store information in various sub-sections of the centralized database;

cross-reference information against an unique identifier for easy retrieval and update; and

retrieve information from the centralized database in response to an inquiry to provide requested information to the user.

19. (withdrawn) A system according to Claim 17 wherein said client system is further configured with:

a displaying component; and

a sending component to send an inquiry to the server system such that the server system can process and download the requested information to the client system, wherein said sending component functions in response to at least one of a click of a mouse button and a voice command.

20. (withdrawn) A system according to Claim 19 wherein said system is further configured to be protected from access by unauthorized individuals and further configured with:

a collection component for collecting information from users into the centralized database;

a tracking component for tracking information on an on-going basis;

a displaying component for displaying various user interfaces;

a receiving component for receiving an inquiry from the client system regarding at least one of a user interface; and

an accessing component for accessing the centralized database and causing the retrieved information to be displayed on the client system.